CLAIMS

We claim:

[c1] 1. A system for sharing a hierarchical document, the hierarchical document having a node, comprising:

a component that receives an indication of a privilege for the node, the privilege indicating access rights for the node, the indication including a holder of the privilege;

a component that receives an access request to the node from a requestor; and

a component that handles the received access request, wherein the handling includes determining whether the requestor is a holder of a privilege that is appropriate for the received access request.

[c2] 2. The system of claim 1 wherein the holder of the privilege is a user.

[c3] 3. The system of claim 2 wherein the holder is an application program.

[c4] 4. The system of claim 2 wherein the holder is an operator of an application program.

[c5] 5. The system of claim 1 wherein the holder is a client computing device.

[c6] 6. The system of claim 1 wherein the system receives an indication of the holder from an operating system.

[c7] 7. The system of claim 1 wherein the system authenticates the holder.

[c8] 8. The system of claim 1 wherein the received access request is a mutation relating to a node.

[c9] 9. The system of claim 8 wherein the indication of an access request indicates the node.

[c10] 10. The system of claim 8 wherein the privilege is appropriate for the received access request when the mutation and privilege are both Insert.

[c11] 11. The system of claim 8 wherein the privilege is appropriate for the received access request when the mutation and privilege are both Update.

[c12] 12. The system of claim 8 wherein the privilege is appropriate for the received access request when the mutation and privilege are both Delete.

[c13] 13. The system of claim 1 wherein the privilege is appropriate for the received access request when the received access request is Read and the privilege is Insert.

[c14] 14. The system of claim 1 wherein the holder holds multiple privileges.

[c15] 15. The system of claim 1 wherein the holder holds the privilege on descendants of the node merely by holding a privilege on the node.

[c16] 16. The system of claim 15 wherein the privilege is Delete.

[c17] 17. The system of claim 1 wherein the holder holds a different privilege on attributes of the node.

[c18] 18. The system of claim 17 wherein the privilege is Insert and the different privilege is Read.

[c19] 19. The system of claim 17 wherein the holder does not hold the privilege on descendants of the node merely by holding the privilege on the node.

[c20] 20. The system of claim 1 wherein the holder does not hold a privilege on a descendant of the node merely by owning the privilege on the node.

[c21] 21. The system of claim 1 wherein the holder holds a different privilege on a parent of the node.

[c22] 22. The system of claim 21 wherein the holder is privileged to request a mutation relating to the parent.

[c23] 23. The system of claim 22 wherein the mutation is to remove the node.

[c24] 24. The system of claim 1 wherein multiple holders hold the privilege.

[c25] 25. The system of claim 1 wherein the holder of the privilege is a privilege group.

[c26] 26. The system of claim 25 wherein the privilege group has multiple members.

[c27] 27. The system of claim 26 wherein the member is an application program.

[c28] 28. The system of claim 26 wherein the member is an operator of an application program.

[c29] 29. The system of claim 26 wherein the member is a client computing device.

[c30] 30. The system of claim 1 wherein the handling includes returning a message comprising an indication of mutations to users of the system.

[c31] 31. The system of claim 30 wherein the message includes only information for which a recipient of the message holds an appropriate privilege.

[c32] 32. A method in a distributed computing environment for sharing a hierarchical document, the hierarchical document having a node, comprising:

receiving an indication of a privilege for the node, the privilege indicating access rights for the node, the indication including a holder of the privilege;

receiving an access request to the node from a requestor; and

handling the received access request, wherein the handling includes determining whether the requestor is a holder of an appropriate privilege for the received access request.

[c33] 33. The method of claim 32 wherein the holder of the privilege is a user.

[c34] 34. The method of claim 33 wherein the holder is an application program.

[c35] 35. The method of claim 33 wherein the holder is an operator of an application program.

[c36] 36. The method of claim 32 wherein the holder is a client computing device.

[c37] 37. The method of claim 32 wherein the system receives an indication of the holder from an operating system.

[c38] 38. The method of claim 32 wherein the system authenticates the holder.

[c39] 39. The method of claim 32 wherein the received access request is a mutation relating to a node.

[c40] 40. The method of claim 39 wherein the indication of an access request indicates the node.

[c41] 41. The method of claim 39 wherein a privilege is appropriate for the received access request when the mutation and privilege are both Read.

[c42] 42. The method of claim 39 wherein a privilege is appropriate for the received access request when the mutation and privilege are both Insert.

[c43] 43. The method of claim 39 wherein a privilege is appropriate for the received access request when the mutation and privilege are both Update.

[c44] 44. The method of claim 39 wherein a privilege is appropriate for the received access request when the mutation and privilege are both Delete.

[c45] 45. The method of claim 39 wherein a privilege is appropriate for the received access request when the mutation is Read and the privilege is Insert.

[c46] 46. The method of claim 32 wherein the holder holds multiple privileges.

[c47] 47. The method of claim 32 wherein the holder holds the privilege on descendants of the node merely by holding a privilege on the node.

[c48] 48. The method of claim 47 wherein the privilege is Delete.

[c49] 49. The method of claim 32 wherein the holder holds a different privilege on attributes of the node.

[c50] 50. The method of claim 49 wherein the privilege is Insert and the different privilege is Read.

[c51] 51. The method of claim 49 wherein the holder does not hold the privilege on descendants of the node merely by holding the privilege on the node.

[c52] 52. The method of claim 32 wherein the holder does not hold a privilege on a descendant of the node merely by owning the privilege on the node.

[c53] 53. The method of claim 32 wherein the holder holds a different privilege on a parent of the node.

[c54] 54. The method of claim 53 wherein the holder is privileged to request a mutation relating to the parent.

[c55] 55. The method of claim 54 wherein the mutation is to remove the node.

[c56] 56. The method of claim 54 wherein the mutation is to remove an attribute.

[c57] 57. The method of claim 32 wherein multiple holders hold the privilege.

[c58] 58. The method of claim 32 wherein the holder of the privilege is a privilege group.

[c59] 59. The method of claim 58 wherein the privilege group has multiple members.

[c60] 60. The method of claim 59 wherein the member is an application program.

[c61] 61. The method of claim 59 wherein the member is an operator of an application program.

[c62] 62. The method of claim 59 wherein the member is a client computing device.

[c63] 63. The method of claim 32 wherein the handling includes returning a message comprising an indication of mutations to users of the system.

[c64] 64. The method of claim 63 wherein the message includes only information for which a recipient of the message holds an appropriate privilege.

[c65] 65. The method of claim 32 wherein the access request identifies the node with a unique identification.

[c66] 66. The method of claim 32 wherein the access request is received as a message.

[c67] 67. The method of claim 66 wherein the message is represented in XML.